An Efficient Traceability Mechanism in the Audited Cloud Data Storage

Authors : Ramya P, Lino Abraham Varghese, S. Bose

Abstract : By cloud storage services, the data can be stored in the cloud, and can be shared across multiple users. Due to the unexpected hardware/software failures and human errors, which make the data stored in the cloud be lost or corrupted easily it affected the integrity of data in cloud. Some mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. But public auditing on the integrity of shared data with the existing mechanisms will unavoidably reveal confidential information such as identity of the person, to public verifiers. Here a privacy-preserving mechanism is proposed to support public auditing on shared data stored in the cloud. It uses group signatures to compute verification metadata needed to audit the correctness of shared data. The identity of the signer on each block in shared data is kept confidential from public verifiers, who are easily verifying shared data integrity without retrieving the entire file. But on demand, the signer of the each block is reveal to the owner alone. Group private key is generated once by the owner in the static group, where as in the dynamic group, the group private key is change when the users revoke from the group. When the users leave from the group the already signed blocks are resigned by cloud service provider instead of owner is efficiently handled by efficient proxy re-signature scheme.
Keywords : data integrity, dynamic group, group signature, public auditing
Conference Title : ICCSE 2015 : International Conference on Computer Science and Engineering
Conference Location : Singapore, Singapore
Conference Dates : September 10-11, 2015